Computer Engineering and Intelligent Systems
ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online)
Vol 3, No.4, 2012

Data Security Using Cryptosteganography in Web Application

Abhishek Patidar Gajendra Jagnade* Laxmi Madhuri Pranay Mehta Ronak Seth

Maharashtra Academy Of Engineering,Alandi,Pune

* E-mail of the corresponding author: praggroup@yahoo.com

Abstract

Data security using Cryptosteganography in web application is a web based application used to conceal important information through hybrid cryptography and Steganography and provide means of its secure transmission through any medium or channel .Using a web browser the user uploads the important information and an envelope image. The same is received by the Data Shielder facade web application .The web application sends the data and envelope image to the real Data Shielder .It generates a unique key and encrypts the crucial data .The key is associated with a "unique id" and preserved in a store .Then the encrypted information is embedded into the envelope image using modified BPCS technique .Finally a stego image is generated .Data Shielder returns the "unique id" and stego image to the facade web application .Web application further archives the stego image and unique key and allows the user to download it. The user can simply unzip the archive and transmit the stego image through unsecured channels like email, sockets, pen drives, cds, dvds, etc. And can keep the unique id safe. When the user wants its data back then user needs to upload the stego image and the "unique id" to the Data Shielder facade web application. The web application sends the unique id and stego image to the real Data Shielder. First it finds the encryption key from the store through the unique id. Next, reversing the BPCS Steganography, the stego image is processed and encrypted data is fetched. Finally using the encryption key decryption is done and the crucial data is fetched back. The same is returned to the facade web application, which is rendered to the user.

Keywords: Cryptography, Steganography, Stego- image, Threshold Value

1. Introduction

Cryptography and Steganography are well known and widely used techniques that manipulate information (messages) in order to cipher or hide their existence respectively. This is a web application which uses combination of Steganography and Cryptography techniques .Steganography is the art and science of communicating in a way which hides the existence of the communication. Cryptography scrambles a message so it cannot be understood. The Steganography hides the message for security. This paper describes a system, which uses both Cryptography and Steganography for better confidentiality and security. Major applications of the project are confidential communication and secret data storage which can be used by normal people to secure their data & for military purpose, government organization, private sector organization for security concern.

So this project aims to provide hybrid means of security and to improve existing BPCS technique for Steganography and to develop new cryptographic algorithm.

2. Basic Concepts and Related Work

There are many aspects to security and many applications. One essential aspect for secure communications is that of cryptography. But it is important to note that while cryptography is necessary for secure communications, it is not by itself sufficient. There are some specific security requirements for cryptography, including Authentication, Privacy/confidentiality, and Integrity Non-repudiation. The three types of algorithms are described:

(i) Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption.

(ii)Public Key Cryptography (PKC): Uses one key for encryption and another for decryption.

(iii)Hash Functions: Uses mathematical transformation to irreversibly "encrypt" information.

Steganography is the other technique for secured communication. It encompasses methods of transmitting a secret message through innocuous cover carriers in such a manner that the very existence of the embedded messages is undetectable. Information can be hidden in images, audio, video, text, or some other digitally representative code. Steganography systems can be grouped by the type of covers used (graphics, sound, text, executables) or by the techniques used to modify the covers

a) Substitution system.

b) Transform domain techniques.

c) Spread spectrum techniques.

d) Statistical method.

e) Distortion techniques.

f) Cover generation methods.

2.1 Architecture

Architecture consists of four basic blocks

1) Encryption : Matrix Mapping Method For Symmetric Key Cryptography
2) Steganography : Modified BPCS
3) Decryption Matrix Mapping Method For Symmetric Key Cryptography
4) Desteganography : Modified BPCS

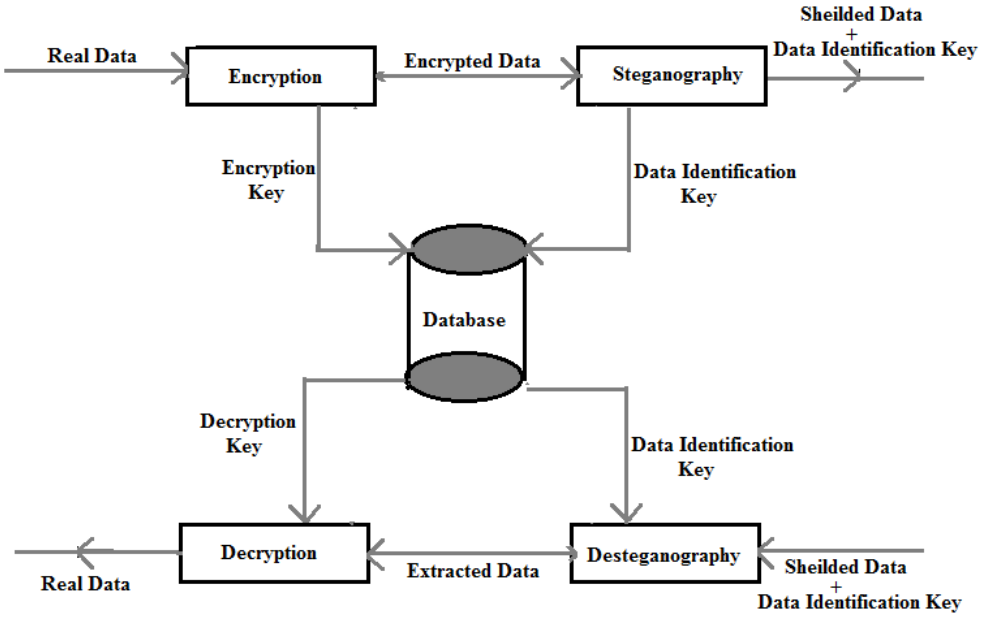

Figure1. Architecture Diagram of System

2.1.1 Encryption: Matrix Mapping Method for Symmetric Key Cryptography

In this algorithm, using the key we generate a mapping matrix. Every byte of the mapping image is unique

and is with respect to key. The mapping matrix is of size 16 by 16.This algorithm is influenced by Applied cryptography in Java (Partida, A.Andina, D.Atos).

Algorithm:

1) The source file is opened for reading in binary mode.

2) Every byte of the source file is read and converted into its equivalent 8-bit binary number.

3) Split the 8-bit binary number into 4-bit higher and lower nibble number.

4) Convert these two 4-bit nibbles into its equivalent decimal value.

5) With the help of these two decimal values pickup a pixel from the mapping matrix. Where higher nibble equivalent decimal value acts as row indicator and lower nibble equivalent decimal value acts as column indicator for mapping image.

6) Replace the original pixel with the byte selected from mapping matrix.

7) Encrypted file gets generated as the above process is repeated for all the pixels.

2.1.2 Steganography: Modified BPCS

Our new Steganography uses an image as the vessel data, and we embed secret information in the bit-planes of the vessel. This technique makes use of the characteristics of the human vision system whereby a human cannot perceive any shape information in a very complicated binary pattern. We can replace all of the “noise-like” regions in the bit-planes of the vessel image with secret data without deteriorating the image quality.This algorithm is influenced by Principle and application of BPCS-Steganography(Eiji Kawaguchi and Richard O.Eason).This algorithm is termed as Modified “BPCS-Steganography,” which stands for Bit-Plane Complexity Segmentation Steganography. Input data will be vessel image and data to embed in byte format. Load the vessel image into memory. Get width and height of the memory image. Generate a threshold value. For each pixel get red, green and blue values of current pixel .

Algorithm:

Real Image and data to Embed in byte array format is given as input.

1) Load the vessel image into memory.

2) Get a "readable pen" for the memory image.

3) Get width and height of the memory image.

4) Generate a threshold value.

5) Loop for all rows of memory image

Loop for all cols of memory image

a) Using the "readable pen" get red, green and blue values of current pixel.

b) if red <= threshold and green <= threshold and blue <= threshold then

* mark the pixel as NOISY (store in a list).

6) If NOISY pixel list size >= size of data to embed go to step 8.

7) Raise Error "Content length is more than embedding capacity of Vessel Image".

8) Convert the Data to embed into SECRET BLOCKS

a) Create a empty list to hold secret blocks

b) Loop for every byte of input data

* conjugate the byte

* store the conjugated byte into secrect block list.

9) Get a "writable pen" for the memory image.

10) Loop for every element of NOISY pixel list

a) Embed 2 bytes of data from SECRET blocks into red, green and blue bands of noisy pixel.

b) Using the writable pen write the pixel into memory image.

11) Write back the memory image into IMAGE FILE.

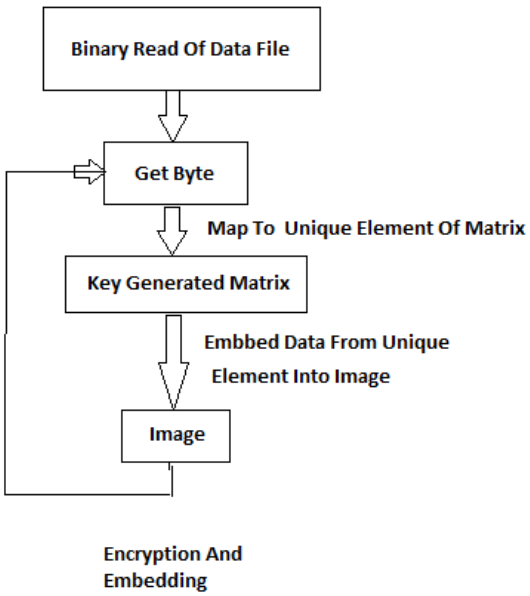

Figure 2: Algorithm to encrypt data and embed it into image

2.1.3 Decryption: Matrix Mapping Method for Symmetric Key Cryptography

In this algorithm, using the key we generate a mapping matrix. Every byte of the mapping image is unique and is with respect to key. The mapping matrix is of size 16 by 16.

Algorithm:

1) The encrypted file is opened for reading in binary mode.

2) Every byte of the encrypted file is read and converted into its equivalent 8-bit binary number.

3) Match the byte in the mapping matrix and find out row and column number of the matched byte.

4) Form 2 nibbles using the row number and column number. Generate a 8-bit binary number from 4-bit higher (row) and lower (column) nibble number.

5) Substitute this generated 8 bit binary data in place of the current byte.

6) Original file gets generated as the above process is repeated for all the pixels.

Get the bytes from image using Desteganography and use the key to generate decryption matrix. Now match the byte which we got from image with each matrix element. And get corresponding row and column number of matched element. Convert the obtained row and column number into binary format. Deconjugate these two numbers which represents original data.

2.1.4Desteganography: Modified BPCS

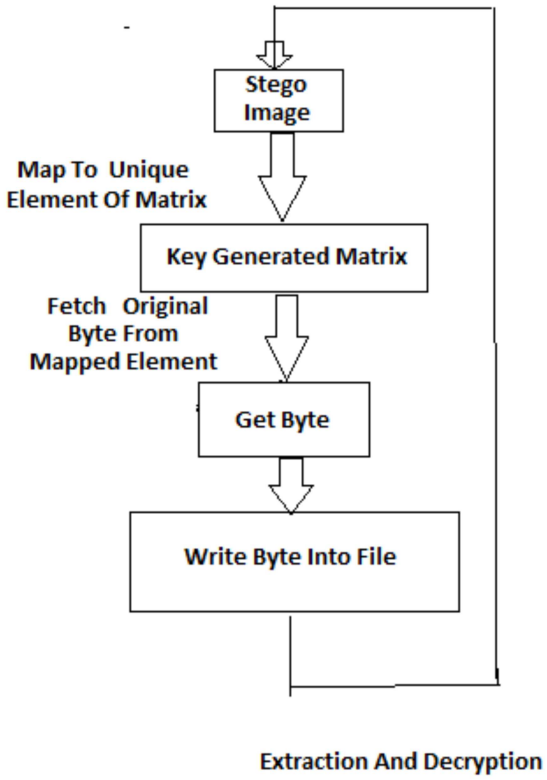

Figure 3. Algorithm to decrypt data and extract from image

Image having embedded data is given as input .

Algorithm:

1) Load the image into memory.

2) Get a "readable pen" for the memory image.

3) Get width and height of the memory image.

4) Generate a threshold value.

5) Loop for all rows of memory image

Loop for all cols of memory image

a) Using the "readable pen" get red, green and blue values of current pixel.

b) If red <= threshold and green <= threshold and blue <= threshold then mark the pixel as NOISY (store in a list)

6) Loop for every element of NOISY pixel list

a) Extract bytes of data from red, green and blue bands of noisy pixel.

b) Deconjugate the secret blocks and form data bytes.

c) Concatenate the data in a result buffer.

7) Write back the result buffer into a FILE Input data will be image having embedded data. Load the image into memory. Get width and height of the memory image. Generate a threshold value.

Conclusion & Future Enhancements

The work accomplished during this project can be summarized with the following points:

1) In this project we have presented a new system for the combination of cryptography and Steganography using matrix mapping method for Symmetric Key Cryptography and modified BPCS technique for Steganography which could be proven a highly secured method for data communication in near future.

2) Steganography especially combined with cryptography, is a powerful tool which enables people to communicate without possible eavesdroppers even knowing there is a form of communication in the first place. The proposed method provides acceptable image quality with very little distortion in the image.

3) The main advantage of this Cryptosteganography System is hybrid combination of cryptography and Steganography which provides double layer security.

In future video or audio files can be used to hide data instead of images.

References

Visual Cryptography Steganography In Images, PiyushMarwaha , PareshMarwaha

A steganography implementation ,Mehboob, B. Faruqui, R.A.

Principle and application of BPCS-Steganography,Eiji Kawaguchi and Richard O.Eason,KIT,Japan

Applied cryptography in Java ,Partida, A.Andina, D.Atos-ODS , S.A.Madrid.

Data Security Using Data Hiding , Moon, S.K. Kawitkar, R.S.,PICT, Pune.

Digital steganography: hiding data within data,Artz, D.;Los Alamos Nat. Lab., NM